124

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/650,211	08/28/2003	Anand Subramaniam	1565.034US3	7162

21186 7590 09/08/2004

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/650,211	SUBRAMANIAM ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *34-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *34-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *08/28/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Cancellation of claims 1-33 has been acknowledged.

2. **Claims 34-53** have been examined.

Drawings

3. The drawings filed on 08/28/ 2003 are accepted by Examiner.

Specification

4. The disclosure is objected to because of the following informalities: please add the phrase "which is now U.S. Patent No.:6,640,302 issued October 28, 2003," after the phrase "on January 28, 2000," line 2 of the specification. Appropriate correction is required.

Information Disclosure Statement PTO-1449

5. The Information Disclosure Statement submitted by applicant on 08/28/2003 has been considered. Please see attached PTO-1449.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude"

granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 34-35, 39, 41, 42, 45, 47, 48, 52, 53 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-25 of U.S. Patent No. 6, 640,302 B1. Although the conflicting claims are not identical, they are not patentably distinct from each other because limitations of claims 34-35, 39, 41, 42, 45, 47, 48, 52 and 53 of instant application are covered and therefore anticipated by claims 1-25 of U.S. Patent No. 6, 640,302 B1. The patent claims the same elements and their functions plus additional elements and their functions not being claimed in the present application. The omission of theses elements and their functions from patent claims would have been anticipated if the functions or the elements are not desired (see MPEP 2144.04(II)A).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. **Claims 34-38, 40-41 and 43-51** are rejected under 35 U.S.C. 102(e) as being anticipated by Birrell et al (5,805,803 A) cited in the Information Disclosure Statement submitted by applicant on 08/28/2003.

As per claim 34 Birrell et al (5,805,803 A) teach a border server **(see fig.1, block 140 corresponds to Applicant's border server)**, comprising: secure connection software for secure communication with a client where the client resides in an insecure network **(see col.3, lines 5-7; fig.1 wherein client computer 110 is located within an insecure network of intranet 120; col.2, lines 22-27 where it disclose conducting secure communications or connections using application layer of the internet protocol stack)**; insecure connection software for communicating with a target server (**where private resource 160 may include a web server 161 as depicted in fig.1 and col.3, lines 17-18 where such a web server may be considered as target server)** where the target server resides in a secure network **(see fig.1 wherein the target server 161, checkers 141, redirector 142 are within secure network communicating to non-secure network through firewall 130; col.4, lines 5-10 where insecure connection software communication is represented by**

HTTP protocol), and a transformer **(see fig.1 block 143 proxy server that corresponds to Applicant's transformer using the block 142 redirector)** to transform a secure request received from the client to an insecure request for the target server, and the transformer also transforms insecure data received from the target server into secure data while the client is authenticated and then sends the secure data to the client computer **(see col.4, lines 5-17 where disclose a redirector supplying a secure URL in response to a client request having a non-secure URL; fig.2, block 142 where it disclose the transformation of non-secure URL to a secure URL; Examiner further refers Applicant to fig.3 wherein at step 330-370 all communication between client 110, checker, and proxy are secured through initial modification of non-secure URL (http) with corresponding secure URL (https). At step 210 the request is send to target computer 160 wherein the communication within secure network no longer is secure communication (also see col.4, lines 52-56) and at step 211 the reverse process takes place by sending a message fro target computer 160 in non-secure communication format to proxy 143 (also see col.4, lines 53-55) and then proxy through the same process of modification of URL send the message in secure communication (https) back to client computer 110 (also see col.4, lines 55-57) Birrel also teach sending secure communication to a client computer if the client computer is authenticated where in last 6 lines of abstract it disclose the secure communication is only being done if a token by authenticated client is valid otherwise the client has to be authenticated. Also see col.4, line 28-36).**

As per claim 35 Birrell et al (5,805,803 A) teach the border server of claim 34, wherein the transformer transforms the secure request, which is a Uniform Resource Locator request, and wherein the secure connection software is used by a browser of the client to issue the secure request **(see col.4, lines 5-17 where disclose a redirector supplying a secure URL in response to a client request having a non-secure URL; also see fug.1, block 111 representing the browser for connection)**.

As per claim 36 Birrell et al (5,805,803 A) teach the border server of claim 34, wherein the transformer transforms the insecure data by sending the insecure data to the client as the secure data using a Hypertext Markup Transfer Protocol over a Secure Sockets Layer (HTTPS) which is used by the secure connection software **(see fig.2, item 202 representing the HTTPS protocol for sending data to client 110; fig.2, block 142 where it disclose the transformation of non-secure URL to a secure URL).**

As per claim 37 Birrell et al (5,805,803 A) teach the border server of claim 34, wherein the target server is indirectly accessible to the client via the transformer while the client remains authenticated **(see fig.1 wherein the target server corresponds to any server such as block 161 that controls the resources 160 are indirectly accessible to client 110 via block 142 redirector under the command of block 143 proxy server that corresponds to Applicant's**

transformer and see col.4, lines 27-46 where the authentication is being done).

As per claim 38 Birrell et al (5,805,803 A) teach the border server of claim 34, wherein the client is authenticated by an authentication system on the secure network **(see col.4, lines 27-46 where the authentication is being done through verification of the client using client information stored in a database within a firewall and using the checker 141 of fig.1 where it reside in secure network area. Examiner also considers the firewall as belonging to the secure part of the network).**

As per claim 40 Birrell et al (5,805,803 A) teach the border server of claim 34 further comprising a redirector that intercepts and redirects the secure requests to the transformer **(see fig.1, block 140 comprises a redirector 142; fig.2, block 142 redirecting to proxy 143 that acts as transformer).**

As per claim 41 Birrell et al (5,805,803 A) teach a method for operating a border server **(see fig.1, block 140 corresponds to Applicant's border server)**, said method comprising: receiving a secure request from a client over an insecure network **(see col.3, lines 5-7; fig.1 wherein client computer 110 is located within an insecure network of intranet 120; col.2, lines 22-27 where it disclose conducting secure communications or connections using application layer of the internet protocol stack and col.4, lines 5-17 where**

disclose a redirector supplying a secure URL in response to a client request having a non-secure URL); transforming the secure request into an insecure request while authenticating the client and sending the insecure request to a target server residing in a secure network; receiving insecure data from the target server; and transforming the insecure data into secure data and sending the secure data to the client over the insecure network, if the client was successfully authenticated **(see fig.1 where private resource 160 may include a web server 161 as depicted in fig.1 and col.3, lines 17-18 where such a web server may be considered as target server; col.4, lines 5-17 where disclose a redirector supplying a secure URL in response to a client request having a non-secure URL; fig.2, block 142 where it disclose the transformation of non-secure URL to a secure URL; Examiner further refers Applicant to fig.3. At step 330-370 all communication between client 110, checker, and proxy are secured through initial modification of non-secure URL (http) with corresponding secure URL (https). At step 210 the request is send to target computer controlling resources 160 wherein the communication within secure network no longer is secure communication (also see col.4, lines 52-56) and at step 211 the reverse process takes place by sending a message from target computer 160 in non-secure communication format to proxy 143 (also see col.4, lines 53-55) and then proxy through the same process of modification of URL send the message in secure communication (https) back to client computer 110 (also see col.4, lines 55-57) Birrel also teach sending secure communication to a**

client computer if the client computer is authenticated where in last 6 lines of abstract it disclose the secure communication is only being done if a token by authenticated client is valid otherwise the client has to be authenticated. Also see col.4, line 28-36).

As per claim 43 Birrell et al (5,805,803 A) teach the method of claim 41 wherein the receiving further includes intercepting, by the border server **(see fig.1, block 140 corresponds to Applicant's border server)**, the secure request sent from the client **(see fig.2 where proxy 143 within border server 140 intercepts the secure request 330),** wherein the secure request was originally directed from the client to the target server **(see fig.2 where the secure request 330 is originated from client 110 to target resource 160 by final request 210 where private resource 160 may include a web server 161 as depicted in fig.1 and col.3, lines 17-18 where such a web server may be considered as target server).**

As per claim 44 Birrell et al (5,805,803 A) teach the method of claim 41 wherein the transforming of the secure request further includes sending the insecure request to the target server within a secure intranet environment, which is the secure network **(see At step 330-370 all communication between client 110, checker, and proxy are secured through initial modification of non-secure URL (http) with corresponding secure URL (https). At step 210 the request**

is send to target computer controlling resources 160 wherein the communication within secure network (also see col.4, lines 52-56)).

As per claim 45 Birrell et al (5,805,803 A) teach the method of claim 41 wherein the transforming of the secure request includes using a directory services database in connection with an authentication system to authenticate the client **(see col.4, lines 32-36 where the authentication using password and id verification includes using a user database that corresponds to Applicant's directory services database inside a firewall).**

As per claim 46 Birrell et al (5,805,803 A) teach the method of claim 41 wherein the transforming of the secure request includes blocking, by the border server, direct access from the client to the target server **(see col.4, lines 5-17 where client request for access to resources are redirected to proxy server 143 and therefore any direct access to target server from client is blocked unless through the proxy server 143 within the border server 140).**

As per claim 47 Birrell et al (5,805,803 A) teach the method of claim 41 wherein the receiving further includes receiving a username and password with the secure request, which is used when authenticating the client **(see col.4, lines 27-37 where authentication is being done using verification of user identification such as user name and password by secure challenge-response authentication).**

As per claim 48 Birrell et al (5,805,803 A) teach a method for operating a border server **(see fig.1, block 140 corresponds to Applicant's border server)**, comprising; intercepting a secure request issued from a client for secure data accessible from a secure network **(see col.4, lines 5-13; fig.3, item 330 the secure request by client 110 for secure data within private resources 160 as depicted in more detailed in fig.1 where the secure data could be data within web server 161 and it is within a secure network since the network 150 that includes the resources is protected by firewall against insecure network such as internet),** wherein the secure request is intercepted from an insecure network **(see fig.3 where the secure request 330 is originated from client 110 which is located within insecure network as depicted further in fig.1; interception is being done by proxy 143 within the border server 140)**; authenticating the client while transforming the secure request into an insecure request within the secure network; and locating the secure data within the secure network and transforming the secure data into insecure data for delivery to the client over the insecure network using secure communications **(see fig.1 where private resource 160 may include a web server 161 as depicted in fig.1 and col.3, lines 17-18 where such a web server may be considered as target server; col.4, lines 5-17 where disclose a redirector supplying a secure URL in response to a client request having a non-secure URL; fig.2, block 142 where it disclose the transformation of non-secure URL to a secure URL; Examiner further refers Applicant to fig.3. At step 330-370 all**

communication between client 110, checker, and proxy are secured through initial modification of non-secure URL (http) with corresponding secure URL (https). At step 210 the request is send to target computer controlling resources 160 wherein the communication within secure network no longer is secure communication (also see col.4, lines 52-56) and at step 211 the reverse process takes place by sending a message from target computer 160 in non-secure communication format to proxy 143 (also see col.4, lines 53-55) and then proxy through the same process of modification of URL send the message in secure communication (https) back to client computer 110 (also see col.4, lines 55-57) Birrel also teach sending secure communication to a client computer if the client computer is authenticated where in last 6 lines of abstract it disclose the secure communication is only being done if a token by authenticated client is valid otherwise the client has to be authenticated).

As per claim 49 Birrell et al (5,805,803 A) teach the method of claim 48 wherein the intercepting further includes intercepting the secure request that was originally directed to a target server having the secure data and located within the secure network **(see fig.3, item 330 where the secure request is intercepted by proxy 143 within the border server 140 and where the request is directed to private resources 160 as secure data within target computer such as block 161 in fig.1 that acts a web server; col.4, lines 5-12).**

As per claim 50 Birrell et al (5,805,803 A) teach the method of claim 48 wherein the locating further includes using Secure Socket Layer protocols as the secure communications over the Internet, which is the insecure network **(see col.5, lines 42-47 where the use of SSL (Secure Socket Layer Protocol) as the means of a communication is disclosed).**

As per claim 51 Birrell et al (5,805,803 A) teach the method of claim 48 wherein the locating further includes issuing the insecure request to a target server within the secure network in order to acquire the secure data **(see fig.3, item 210 representing insecure request to private resources 160 and where in fig.1 private resources 160 includes a web server 161 that corresponds to Applicant's target server; and where the web server 161 of fig.1 is located within the secure network 150 protected by firewall 130 in cooperation with tunnel or border server 140).**

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 39, 42 and 52-53** are rejected under 35 U.S.C. 103(a) as being unpatentable over Birrell et al (5,805,803 A) in view of Nozaki (6,128,644 A).

As per claims 39, 42, 52 and 53 Birrell et al (5,805,803 A) teach all limitation of the claims as applied to claims 34, 41 and 48 but do not disclose explicitly the transformer maintains a cache having the secure data for servicing subsequent requests for the secure data, checking cache for stored secure/insecure data and accessibility from the secure network or target server. However Nozaki (6,128,644 A) disclose a client system which is capable of having processing using a typical WWW browser (see col.3, lines 5-8) having the transformer maintains a cache having the secure data for servicing subsequent requests for the secure data, checking cache for stored secure/insecure data and accessibility from the secure network or target server **(see col.6, lines 41-46 where it disclose the proxy server that corresponds to Applicant's transformer have caching capability in order to give access to static files retrieved from the web server upon subsequent request for the resources from www server or web server within a secure network since it disclose some proxy server have security management such as firewall).** It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Nozaki's proxy caching capabilities in Birrel's proxy server that corresponds to Applicant's transformer in order to give access to static files retrieved from a resource upon receiving request for these resources.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. U.S.Patent No. US (6,745,229 B1) teach web based integrated customer interface for invoice reporting.

b. U.S.Patent No. US (6,065,120 A) teach method and system for self-provisioning a rendezvous to ensure secure access to information in a database from multiple devices.

c. U.S.Patent No. US (6,233,608 B1) teach method and system for securely interacting with managed data from multiple devices.

d. U.S.Patent No. US (6,148,405 A) teach method and system for secure lightweight transactions in wireless data networks.

e. U.S.Patent No. US (6,263,437 B1) teach method and apparatus for conducting crypto-ignition processes between thin client devices and server devices over data networks.

f. U.S.Patent No. US (6,233,577 B1) teach centralized certificate management system for two-way interactive communication devices in data networks.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone

number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

09/01/04